REPLACEMENT CLAIMS

1. (cancelled) A method for transmitting a message between a sender user associated with a first e-mail firewall and a recipient user associated with a second e-mail firewall, the method comprising:

intercepting a plurality of data packets associated with a message from the sender user intended for the recipient user, said data packets generated by a process outside of said first e-mail firewall;

assembling said data packets to an application level message;

searching an encryption directory for an entry associated with the second e-mail firewall associate with the recipient user;

retrieving an encryption key associated with the second e-mail firewall, the second e-mail firewall associated with a plurality of recipient users;

encoding the application level message with the encryption key of the second e-mail firewall to provide an encrypted message; and

allowing the encrypted application level message to proceed to said recipient user.

2. (cancelled) The method of Claim 1, wherein said encoding the message is by employing an encryption key that is stored locally by the first e-mail firewall.
3. (cancelled) The method of Claim 1, wherein said encoding the message is by employing an encryption key that is retrieved from an external server.
4. (cancelled) The method of Claim 3, wherein retrieving the key from an external server is over a secure communication link.
5. (cancelled) The method of Claim 4, wherein the secure communication link is by employing a locally stored encryption key associated with the external server.
6. (cancelled) A method for receiving a message by a recipient user associated with a second e-mail firewall from a sender user associated with a first e-mail firewall, the first e-mail firewall encoding the message by using an encryption key of the second e-mail firewall, comprising:

intercepting a plurality of data packets associated with the message by the second e-mail firewall, the second e-mail firewall associated with a plurality of recipient users, said recipient user associated with a process outside of said second e-mail firewall;

assembling said data packets to an application level message;

decoding the application level message with a private key of the second e-mail firewall; and

allowing the decoded application level message to proceed to the recipient user.

7. (currently amended) A method for controlling e-mail message transmission across an e-mail firewall, the e-mail firewall interposed between an internal network associated with ~~an organization~~ a first policy and an external network, the method comprising:

intercepting a plurality of data packets associated with a message from a sender user associated with the internal network, the message directed to a recipient user associated with an external network;

assembling said data packets to an application level message;

filtering the application level message by examining textual content associated with the application level message by employing content filter conditions of the ~~associated organization~~ first policy to provide a filtering result; and

restricting the transmission of the application level message in accordance with said filtering result.

8. (original) The method of Claim 7, wherein said filtering is by parsing the text of the message in accordance with said filter conditions.

9. (original) The method of Claim 8, wherein said parsing of text is by searching for keywords in the text.

10. (original) The method of Claim 8, wherein said parsing of text is by searching for word patterns in the text.

11. (original) The method of Claim 10, wherein said filter conditions employ Boolean expressions.

12. (original) The method of Claim 7, wherein said filtering conditions include rejecting all executable attachments.

13. (original) The method of Claim 7, wherein said filtering conditions include requiring executable attachments to include digital signatures.

14. (original) The method Claim 13, further comprising filtering executable attachments by reference to a directory of trusted signatures.

15. (original) The method of Claim 7, wherein said restricting the transmission includes routing the message in accordance with user defined routing policies.

16. (currently amended) An e-mail control system for filtering e-mail communication transmitted from an internal site associated with ~~an organization~~ a first policy to a plurality of external sites, the e-mail control system interposed between a public network and a private network associated with said internal site, the e-mail control system comprising:

a policy manager, the policy manager intercepting a plurality of data packets associated with an e-mail message transmitted from a user associated with said internal site to at least one user associated with said external site, the policy manages assembling the data packets to an application level message, the policy manager applying at least one policy imposed by the ~~organization~~ first policy to said application level e-mail message by reference to textual content associated with said application level e-mail message; and

a security manager coupled to the policy manager, the security manager adapted to process said application level e-mail message in accordance with policy results received from said policy manager, the security manager facilitating the transmission of said application level e-mail message to the user associated with said external site in response to predetermined organizational policy results from said policy manager.

17. (currently amended) An e-mail control system for filtering e-mail communication received by an internal site associated with ~~an organization~~ a first policy from an external site, the e-mail control system interposed between a public network and a private network associated with said internal site, the e-mail control system comprising:

a policy manager, the policy manager intercepting a plurality of data packets associated with an e-mail message transmitted to a user associated with said internal site from a user associated with said external site, the policy manages assembling the data packets to an application level message, the policy manager applying at least one ~~policy~~ condition imposed by the ~~organization~~ first policy to said application level e-mail message by reference to properties of the application level e-mail message; and

a security manager coupled to the policy manager, the security manager adapted to process said application level e-mail message in accordance with policy results received from said policy manager, the security manager facilitating the transmission of said application level e-mail message to the user associated with said internal site in response to ~~predetermined organizational~~ policy results from said policy manager.

18. (currently amended) A method for filtering e-mail communication between an internal site associated with ~~an organization~~ a first policy and one or more external sites, comprising:

intercepting a plurality of data packets associated with an e-mail message transmitted between an internal site and an external site, the intercepting comprising suspending a transmission flow of said e-mail message between said internal site and said external site, the e-mail message associated with at least one recipient;

assembling said data packets to an application level message;

applying at least one policy imposed by the ~~organization~~ first policy to said application level message e-mail message by reference to textual content associated with said application level e-mail message; and

processing said application level e-mail message in accordance with policy results received from said policy manager, said processing including sending said application level e-mail message to said at least one recipient in response to ~~predetermined organizational~~ policy results from said policy manager.

19. (previously added) The method of Claim 18, wherein said policy refers to a sender address.

20. (previously added) The method of Claim 18, wherein said policy refers to a recipient address.

21. (currently amended) The method of Claim 18, wherein said policy refers to content in the application level e-mail message body.

22. (currently amended) The method of Claim 18, wherein said policy refers to a message header of said application level e-mail message.

23. (previously added) The method of Claim 18, wherein said processing said intercepted e-mail includes an action from the group consisting of pass, quarantine, re-route, return to sender, and send notification.

24. (currently amended) A method for filtering e-mail messages transmitted from an external site to an internal site associated with ~~an organization~~ a first policy, comprising:

intercepting a plurality of data packets associated with an e-mail message having a sender address associated with an external site;

assembling said data packets to an application level message;

extracting at least one recipient address from a recipient address field of the application level e-mail message;

determining whether the [a] first policy ~~imposed by the organization~~ is applicable to said application level message by reference to said extracted recipient address;

applying at least one ~~organizational policy~~ condition from said first policy to said application level e-mail message when said determining provides that said ~~at least one~~ first policy is applicable to said application level e-mail message, said ~~organizational policy~~ condition referring to textual content associated with said application level e-mail message, said applying providing a policy application result; and

processing said application level e-mail message in accordance with said ~~organizational~~ policy application result.

25. (cancelled) A method for providing secure e-mail communication between a first organization and a second organization, comprising:

interposing a first e-mail firewall between a first e-mail server of said first organization and a public network;

interposing a second e-mail firewall between a second e-mail server of said second organization and a public network;

the first e-mail firewall intercepting a plurality of data packets associated with an e-mail message from a sender associated with said first e-mail server to a recipient associated with said second e-mail server, said data packets generated by a process outside of said first e-mail firewall;

the first e-mail firewall assembling said data packets to an application level message;

the first e-mail firewall encrypting said application level e-mail message with a public key of the second e-mail firewall;

the first e-mail firewall transmitting said encrypted application level e-mail message to said recipient;

the second e-mail firewall intercepting said encrypted application level e-mail message prior to receipt by said second e-mail server;

the second e-mail firewall decrypting said encrypted application level e-mail message with a private key of the second e-mail firewall; and

the second e-mail firewall transmitting said decrypted application level e-mail message to said recipient, said recipient associated with a process outside of the second e-mail firewall.

26. (cancelled) The method of Claim 25, further comprising providing a first access firewall between said first e-mail firewall and said public network and further providing a second access firewall between said second e-mail firewall and said public network.

27. (cancelled) The method of Claim 17, wherein said properties of the application level e-mail message comprise whether the application level e-mail message has been encrypted by employing an encryption key.

28. (cancelled) The method of Claim 17, wherein said properties of the application level e-mail message comprise whether the application level e-mail message includes a digital signature.

29. (new) A method for filtering e-mail messages transmitted from an external site to an internal site associated with a first policy, comprising:

intercepting a plurality of data packets associated with an e-mail message having a sender address associated with an external site;

assembling said data packets to an application level message;

detecting whether the application level message includes a digital signature attachment;

applying at least one policy condition to said application level e-mail message, said policy condition applied by reference to said attached digital signature, said applying providing a policy application result; and

processing said application level e-mail message in accordance with said application result.

30. (new) The method of Claim 29, further comprising applying at least a second policy condition to said application level e-mail message in response to a predetermined condition of the attached digital signature.

31. (new) The method of Claim 30, wherein said predetermined condition comprises detecting that the digital signature is a valid digital signature.

32. (new) The method of Claim 31, further comprising selecting the second policy condition by reference to an identity associated with the valid digital signature.

33. (new) the method of Claim 30, wherein the second policy condition detects whether the attached signature is associated with a domain which is included in a stored list of trusted domains.